WALTER BAUR

Decidability and undecidability of theories of abelian groups with predicates for subgroups

Compositio Mathematica, tome 31, nº 1 (1975), p. 23-30
<http://www.numdam.org/item?id=CM_1975__31_1_23_0>

COMPOSITIO MATHEMATICA, Vol. 31, Fasc. 1, 1975, pag. 23–30
Noordhoff International Publishing
Printed in the Netherlands

DECIDABILITY AND UNDECIDABILITY OF THEORIES OF ABELIAN GROUPS WITH PREDICATES FOR SUBGROUPS

Walter Baur[1]

0. Introduction

Let $n > 1$, $k \leqq 5$ be natural numbers and let $T(n, k)$ be the first-order theory of the class of all structures $\langle A, A_0, \cdots, A_{k-1} \rangle$ where A is an n-bounded abelian group (i.e. $nA = 0$) and $A_0, \cdots, A_{k-1}$ are arbitrary subgroups of A. In the present paper the following results concerning decidability of $T(n, k)$ are obtained: (i) $T(n, 5)$ is undecidable, (ii) if n contains a square then $T(n, 4)$ is undecidable, (iii) if n is squarefree then $T(n, 3)$ is decidable. A trivial consequence of (ii) is that the theory of abelian groups with four distinguished subgroups is undecidable[2]

Terminology: 'group' means 'abelian group' except where stated otherwise. 'Countable' means 'finite or countably infinite'. For all undefined notions from logic we refer to [5].

1. Undecidability

The first-order language L of abelian groups consists of a binary function symbol $+$ and a constant 0. Let f_0, f_1 be two unary function symbols and put $L_1 = L \cup \{f_0, f_1\}$. For $n \geqq 1$ let $T_1(n)$ denote the theory of all structures $\langle A, f_0, f_1 \rangle$ where A is an n-bounded abelian group and f_0, f_1 are arbitrary automorphisms of A.

THEOREM 1: *$T_1(n)$ is undecidable for all $n > 1$.*

PROOF: Let G be a (noncommutative) finitely presented 2-generator group with undecidable word problem (see e.g. Higman [2]). Assume

[1] Supported by Schweizerischer Nationalfonds.
[2] See postscript.

that G is the quotient of the free group on the generators f_0, f_1 modulo the normal subgroup generated by $t_0, \cdots, t_{m-1}$ where each t_μ is a word in $f_0, f_1, f_0^{-1}, f_1^{-1}$.

Consider f_0^{-1}, f_1^{-1} as new function symbols and let $T_2(n)$ be the theory in the language $L_1 \cup \{f_0^{-1}, f_1^{-1}\}$ obtained from $T_1(n)$ by adding

$$\forall x(f_0 f_0^{-1}(x) = f_1 f_1^{-1}(x) = x)$$

as a new axiom. $T_2(n)$ is an extension by definitions of $T_1(n)$ and therefore it suffices to show that $T_2(n)$ is undecidable.

Since G has undecidable word problem it suffices to show that for any word t in $f_0, f_1, f_0^{-1}, f_1^{-1}$ the following two statements are equivalent

(i) $T_2(n) \vdash \forall x(\bigwedge_{\mu<m} t_\mu(x) = x) \rightarrow \forall x(t(x) = x)$,

(ii) $t = e$ in G (e is the neutral element of G).

Clearly (ii) implies (i). To prove the other direction assume $t \neq e$ in G. Let $\mathbb{Z}$ be the ring of integers and put $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Let A be the additive group of the group ring $\mathbb{Z}_n[G]$ and define two automorphisms of A by $f_i^A(a) = f_i \cdot a$ ($i = 0, 1$). Let $\mathfrak{A}$ be the unique expansion of $\langle A, f_0^A, f_1^A \rangle$ to a model of $T_2(n)$. Since G operates faithfully on A we have $\mathfrak{A} \models \exists x(t(x) \neq x)$, but clearly $\mathfrak{A} \models \forall x(\bigwedge_{\mu<m} t_\mu(x) = x)$. Hence (i) does not hold and Theorem 1 is proved.

Let $P_0, \cdots, P_4$ be five unary predicate symbols. For $n \geqq 1$ and $k \leqq 5$ let $T(n, k)$ denote the $L \cup \{P_0, \cdots, P_{k-1}\}$-theory of all structures $\langle A, A_0, \cdots, A_{k-1} \rangle$ where A is an n-bounded group and $A_0, \cdots, A_{k-1}$ are arbitrary subgroups of A.

THEOREM 2:

(i) *$T(n, 5)$ is undecidable for all $n > 1$,*

(ii) *if n contains a square then $T(n, 4)$ is undecidable.*

PROOF: (i) By Theorem 1 it suffices to give a faithful interpretation of $T_1(n)$ in a finite extension $T'(n)$ of $T(n, 5)$. $T'(n)$ is obtained from $T(n, 5)$ by adding the following new axioms

(1) $\forall x \exists ! y \exists ! z(P_3(y) \ \& \ P_4(z) \ \& \ x = y+z)$,

(2) $\forall y(P_3(y) \rightarrow \exists ! z(P_4(z) \ \& \ P_i(y+z)))$ $\quad (i \leqq 2)$,

(3) $\forall z(P_4(z) \rightarrow \exists ! y(P_3(y) \ \& \ P_i(y+z)))$ $\quad (i \leqq 2)$.

A model of $T'(n)$ is nothing else than an n-bounded group A together with a direct sum decomposition $A = A_3 \oplus A_4$ and the graphs of three isomorphisms between A_3 and A_4.

Rather than giving the formal details of the interpretation we show how to get a model of $T_1(n)$ out of a model of $T'(n)$ and that we get all models of $T_1(n)$ in this way.

Let $\mathfrak{A} = \langle A, A_0, \cdots, A_4 \rangle$ be a model of $T'(n)$. The axioms of $T'(n)$ guarantee that the maps $g_0, g_1 : A_3 \to A_3$ defined by

$$g_i(a) = a' \Leftrightarrow \mathfrak{A} \models P_3(a) \;\&\; P_3(a') \;\&\; \exists z(P_4(z) \;\&\; P_i(a+z) \;\&\; P_2(a'+z)) \qquad (i = 0, 1)$$

are well-defined automorphisms of A_3. Therefore $\langle A_3, g_0, g_1 \rangle$ is a model of $T_1(n)$.

Conversely assume that $\mathfrak{B} = \langle B, g_0, g_1 \rangle$ is a model of $T_1(n)$. Define $A = B \oplus B$, $A_0 = \text{graph}\,(g_0)$, $A_1 = \text{graph}\,(g_1)$, $A_2 = \{\langle b, b \rangle | b \in B\}$, $A_3 =$ left copy of B in A, $A_4 =$ right copy of B in A. Obviously $\mathfrak{A} = \langle A, A_0, \cdots, A_4 \rangle$ is a model of $T'(n)$ and the model of $T_1(n)$ associated with $\mathfrak{A}$ in the way described above is isomorphic to $\mathfrak{B}$.

(ii) Let p be a prime number such that $p^k | n$ and $p^{k+1} \nmid n$ for some $k > 1$. We interprete $T'(p)$ faithfully in a finite extension T of some extension by definition of $T(n, 4)$. Let T be the theory obtained from $T(n, 4)$ by adding (2), (3) and

(4) $\forall x(P_4(x) \leftrightarrow (p^{k-1} | x \;\&\; px = 0))$,

(5) $\forall x((P_3(x) \;\&\; P_4(x)) \to x = 0)$.

Let $\langle A, A_0, \cdots, A_4 \rangle$ be a model of T. $B = A_3 \oplus A_4$ can be considered as a subgroup of A, by axiom (5). From (2), (3), (4) it follows that

$$\langle B, A_0 \cap B, A_1 \cap B, A_2 \cap B, A_3, A_4 \rangle$$

is a model of $T'(p)$.

Conversely assume that $\mathfrak{B} = \langle B, B_0, \cdots, B_4 \rangle$ is a model of $T'(p)$. Embed B_4 in a direct sum A' of cyclic groups of order p^k such that $B_4 = p^{k-1}A'$ and consider B in the obvious way as a subgroup of $A = B_3 \oplus A'$. Then

$$\mathfrak{A} = \langle A, B_0, B_1, B_2, B_3, B_4 \rangle$$

is a model of T and the model of $T'(p)$ associated with $\mathfrak{A}$ in the way described above is isomorphic to $\mathfrak{B}$. Again it should be clear now how the interpretation works.

Since $T(4, 4)$ is a finite extension of the theory of abelian groups with four predicates for subgroups we obtain

Corollary 1[1]: *The theory of abelian groups with four predicates denoting subgroups is undecidable.*

Kozlov and Kokorin [4] showed that the theory of torsionfree abelian groups with one predicate denoting a subgroup is decidable. The next corollary answers a question of [4]. It follows from the fact that every group is a quotient of a torsionfree group.

Corollary 2[1]: *The theory of torsionfree groups with five predicates denoting subgroups is undecidable.*

2. Decidability

This section is devoted to the proof of the following

Theorem 3: *If n is a squarefree positive number then $T(n, 3)$ is decidable.*

Assume $n = p_0 \cdots p_{k-1} > 1$ squarefree, p_i prime. (If $n = 1$ the theorem is obvious). Since every model $\mathfrak{A}$ of $T(n, 3)$ is a direct product $\mathfrak{A} = \prod_{i<k} \mathfrak{A}_i$ where $\mathfrak{A}_i$ is a model of $T(p_i, 3)$ (see e.g. Kaplansky [3]) it suffices to prove that $T(p, 3)$ is decidable for any prime number p, by the Feferman-Vaught-Theorem [1].

Let p be an arbitrary prime number fixed for the rest of the paper. A model of $T(p, 3)$ is nothing else than a vectorspace U over the field K with p elements together with three subspaces U_0, U_1, U_2. In the following 'vectorspace" always means 'vectorspace over K'. Before starting with the proof we introduce some terminology.

Let U be a subspace of the vectorspace V and let $B = (x_\alpha)_{\alpha<\lambda}$ (λ an ordinal) be a sequence of elements $x_\alpha \in V$. We say that B is linearly independent over U (a basis of V/U resp.) if the sequence $(x_\alpha + U)_{\alpha<\lambda}$ is linearly independent in V/U (a basis of V/U resp.). Let $B' = (x'_\alpha)_{\alpha<\lambda'}$ be another sequence from V. $B \cup B'$ denotes the sequence $(y_\alpha)_{\alpha<\lambda+\lambda'}$ where $y_\alpha = x_\alpha$ if $\alpha < \lambda$ and $y_{\lambda+\alpha} = x'_\alpha$ if $\alpha < \lambda'$.

With any countable model $\mathfrak{A} = \langle U, U_0, U_1, U_2 \rangle$ of $T(p, 3)$ we associate nine vectorspaces $V_0, \cdots, V_7, V$ as follows.

$$V_0 = U/U_0 + U_1 + U_2$$

$$V_1 = U_0 + U_1 + U_2/U_1 + U_2$$

$$V_2 = U_0 + U_1 + U_2/U_0 + U_2$$

[1] See postscript.

$$
\begin{aligned}
V_3 &= U_0+U_1+U_2/U_0+U_1\\
V_4 &= U_0 \cap U_1/U_0 \cap U_1 \cap U_2\\
V_5 &= U_0 \cap U_2/U_0 \cap U_1 \cap U_2\\
V_6 &= U_1 \cap U_2/U_0 \cap U_1 \cap U_2\\
V_7 &= U_0 \cap U_1 \cap U_2\\
V &= U_0 \cap (U_1+U_2)/(U_0 \cap U_1+U_0 \cap U_2)
\end{aligned}
$$

For $i < 8$ put $\kappa_i = \dim V_i$, $\kappa_8 = \kappa_9 = \dim V$, $\mathrm{Inv}(\mathfrak{A}) = \langle \kappa_0, \cdots, \kappa_8 \rangle$.

Let $B_0 = (x_{0,\alpha})_{\alpha<\kappa_0}, \cdots, B_7 = (x_{7,\alpha})_{\alpha<\kappa_7}$, $B = (x_\alpha)_{\alpha<\kappa_8}$ be sequences from U such that

(1) B_i is a basis of V_i $(i < 8)$,

(2) B is a basis of V,

(3) $B_{i+1} \subseteq U_i$ for $i < 3$.

Clearly such sequences exist. For every $\alpha < \kappa_8$ choose $x_{8,\alpha} \in U_1, x_{9,\alpha} \in U_2$ such that $x_\alpha = x_{8,\alpha}+x_{9,\alpha}$. This is possible since $B \subseteq U_1+U_2$. Put $B_8 = (x_{8,\alpha})_{\alpha<\kappa_8}$ and $B_9 = (x_{9,\alpha})_{\alpha<\kappa_9}$.

LEMMA 1:
(i) $B_0 \cup \cdots \cup B_9$ *is a basis of* U,
(ii) $B_1 \cup B_4 \cup B_5 \cup B_7 \cup B$ *generates* U_0,
(iii) $B_2 \cup B_4 \cup B_6 \cup B_7 \cup B_8$ *generates* U_1,
(iv) $B_3 \cup B_5 \cup B_6 \cup B_7 \cup B_9$ *generates* U_2.

PROOF: First we show that $B_0 \cup \cdots \cup B_9$ is linearly independent. Let

$$(*) \qquad \sum_{i \leqq 9} y_i = 0$$

where $y_i = \sum_{\alpha<\kappa_i} a_{i\alpha} x_{i\alpha}$ and $a_{i\alpha} = 0$ for all but finitely many α. We have to show that $a_{i\alpha} = 0$ for all $i \leqq 9$, all $\alpha < \kappa_i$.

Since all summands in (*) except possibly y_0 lie in $U_0+U_1+U_2$ we obtain $a_{0,\alpha} = 0$ for all $\alpha < \kappa_0$, by linear independence of B_0 over $U_0+U_1+U_2$.

Since the remaining summands except possibly y_1 lie in U_1+U_2 we conclude $a_{1,\alpha} = 0$ for all $\alpha < \kappa_1$ as above.

Next note that $y_8 \in U_0+U_2$ by construction of the $x_{8,\alpha}$'s. Therefore all the remaining summands except possibly y_2 lie in U_0+U_2 and hence $a_{2,\alpha}=0$ for all $\alpha<\kappa_2$. $a_{3,\alpha}=0$ is shown in a similar way.

(*) now looks as follows

$$y_4+y_5+y_6+y_7+\sum a_{8,\alpha}x_{8,\alpha}+\sum a_{9,\alpha}x_{9,\alpha} = 0.$$

Replacing $x_{8,\alpha}$ by $x_\alpha - x_{9,\alpha}$ we obtain

$$\sum a_{8,\alpha}x_\alpha+y_4+y_5+y_7 = \sum (a_{8,\alpha}-a_{9,\alpha})x_{9,\alpha}-y_6.$$

The right hand side lies in U_2 whereas the left hand side lies in U_0. Since $y_4+y_5+y_7$ lies in $U_0\cap U_1+U_0\cap U_2$ we obtain

$$\sum a_{8,\alpha}x_\alpha \in U_0\cap U_1+U_0\cap U_2.$$

Hence $a_{8,\alpha}=0$ for all $\alpha<\kappa_8$ by linear independence of B over $U_0\cap U_1+U_0\cap U_2$. $a_{9,\alpha}=0$ is shown in a similar way.

The proof that the remaining $a_{i\alpha}$'s are $=0$ is left to the reader.

Next we prove (iii). Obviously the subspace generated by the B_i's mentioned in (iii) is contained in U_1. Let $y\in U_1$. Since B_2 is a basis of V_2 and $B_2\subseteq U_1$ there exists a linear combination y_2 of the $x_{2,\alpha}$'s such that $y-y_2\in U_1\cap(U_0+U_2)$. Write $y-y_2=z_0+z_2$ where $z_0\in U_0$, $z_2\in U_2$. Note that $z_0\in U_0\cap(U_1+U_2)$. Since B is a basis of V there exists a linear combination $\sum_\alpha a_\alpha x_\alpha$ such that

$$z_0-\sum a_\alpha x_\alpha = u+u'$$

for some $u\in U_0\cap U_1$, $u'\in U_0\cap U_2$. Put $y_8=\sum a_\alpha x_{8,\alpha}$. Since

$$x_\alpha = x_{8,\alpha}+x_{9,\alpha}$$

we obtain

$$\begin{aligned} y-y_2-y_8 &= z_0-y_8+z_2 \\ &= u+(u'+\sum a_\alpha x_{9,\alpha}+z_2). \end{aligned}$$

The expression in the bracket clearly lies in U_2. Since u and the left hand side both lie in U_1 we conclude

$$y-y_2-y_8 \in U_0\cap U_1+U_1\cap U_2.$$

This together with the trivial fact that $B_4 \cup B_6 \cup B_7$ generates $U_0 \cap U_1 + U_1 \cap U_2$ implies (iii).

(iv) is shown in a similar way and (ii) is obvious. (i) follows from what has been proved above and the fact that B_0 is a basis of V_0.

LEMMA 2: *Let* $\mathfrak{A} = \langle U, U_0, U_1, U_2\rangle$, $\mathfrak{A}' = \langle U', U_0', U_1', U_2'\rangle$ *be countable models of* $T(p, 3)$. *Then* $\mathfrak{A} \cong \mathfrak{A}'$ *if and only if* $\mathrm{Inv}(\mathfrak{A}) = \mathrm{Inv}(\mathfrak{A}')$.

PROOF: Clearly $\mathfrak{A} \cong \mathfrak{A}'$ implies that $\mathfrak{A}$, $\mathfrak{A}'$ have the same invariants.

Conversely assume $\mathrm{Inv}(\mathfrak{A}) = \mathrm{Inv}(\mathfrak{A}')$. Choose sequences $B_0, \cdots, B_7, B$ in $\mathfrak{A}$($B_0', \cdots, B_7', B'$ in $\mathfrak{A}'$) such that (1), (2), (3) before Lemma 1 hold. Form B_8, B_9 (B_8', B_9') according to the instructions before Lemma 1. Note that $\mathrm{length}(B_i) = \mathrm{length}(B_i')$ for all $i \leqq 9$ because of $\mathrm{Inv}(\mathfrak{A}) = \mathrm{Inv}(\mathfrak{A}')$. Define a map f from the union of the B_i's onto the union of the B_i''s by mapping the α^{th} elements of B_i onto the α^{th} element of B_i'. By (i) of Lemma 1 f extends to an isomorphism $g : U \to U'$. Since $g(B) = B'$ by construction, it follows from Lemma 1 that $g(U_i) = U_i'$, $i \leqq 2$.

LEMMA 3: *For any 9-tuple* $\langle \kappa_0, \cdots, \kappa_8\rangle$ *of cardinals* $\kappa_i \leqq \omega$ *there exists a countable model* $\mathfrak{A}$ *of* $T(p, 3)$ *such that* $\mathrm{Inv}(\mathfrak{A}) = \langle \kappa_0, \cdots, \kappa_8\rangle$.

PROOF: Let $V_0, \cdots, V_9$ be vectorspaces such that $\dim V_i = \kappa_i$ if $i \leqq 8$, $\dim V_9 = \kappa_8$. Choose a basis $(x_\alpha)_{\alpha<\kappa_8}$ of V_8 and a basis $(y_\alpha)_{\alpha<\kappa_8}$ of V_9. Put $U = \bigoplus_{i \leqq 9} V_i$ and consider the V_i's in the obvious way as subspaces of U. Let V be the subspace of U generated by $\{x_\alpha + y_\alpha | \alpha < \kappa_8\}$ and put

$$
\begin{aligned}
U_0 &= V_1 + V_4 + V_5 + V_7 + V, \\
U_1 &= V_2 + V_4 + V_6 + V_7 + V_8, \\
U_2 &= V_3 + V_5 + V_6 + V_7 + V_9.
\end{aligned}
$$

A straightforward computation shows that $\mathrm{Inv}(\langle U, U_0, U_1, U_2\rangle) = \langle \kappa_0, \cdots, \kappa_8\rangle$.

PROOF OF THEOREM 3: Let φ_{in} ($i < 9$, $n \in \omega$) be $L \cup \{P_0, P_1, P_2\}$-sentences such that for any model $\mathfrak{A}$ of $T(p, 3)$ the following holds

$$\mathfrak{A} \models \varphi_{in} \Leftrightarrow \dim V_i \geqq n \qquad (i < 8, n \in \omega),$$

$$\mathfrak{A} \models \varphi_{8,n} \Leftrightarrow \dim V \geqq n \qquad (n \in \omega).$$

Such sentences can be constructed without difficulties. $\varphi_{0,n}$ e.g. looks as follows

$$\exists x_0, \cdots, x_{n-1} \forall y_0, y_1, y_2 (P_0(y_0) \;\&\; P_1(y_1) \;\&\; P_2(y_2) \rightarrow \bigwedge_{\substack{0 \leqq r_\nu < p \\ \langle r_0, \cdots, r_{n-1} \rangle \neq 0}} \sum_{\nu < n} r_\nu x_\nu \neq y_0 + y_1 + y_2).$$

In order to prove Theorem 3 it suffices to show that the set of all sentences φ which are consistent with $T(p, 3)$ is recursively enumerable.

For any 9-tuple $\vec{\kappa} = \langle \kappa_0, \cdots, \kappa_8 \rangle$ of cardinals $\kappa_i \leqq \omega$ put

$$T_{\vec{\kappa}} = T(p, 3) \cup \{\varphi_{in} | i < 9, n \leqq \kappa_i\} \cup \{\neg\, \varphi_{i, \kappa_i + 1} | \kappa_i < \omega\}.$$

Note that $T_{\vec{\kappa}}$ is consistent and $\aleph_0$-categorical, by Lemmas 2, 3. Therefore φ is consistent with $T(p, 3)$ if and only if φ holds in some countable model of $T(p, 3)$ if and only if there exists a $\vec{\kappa}$ such that $T_{\vec{\kappa}} \vdash \varphi$. This proves Theorem 3.

REMARK: If p is a prime number then $T(p, 3)$ is decidable whereas $T(p, 5)$ is undecidable.

Question: Is $T(p, 4)$ decidable?

Postscript: $T(p^9, 1)$ is undecidable (to appear in Proc. Amer. Math. Soc.).

REFERENCES

[1] S. FEFERMAN and R. L. VAUGHT: The first order properties of algebraic systems, *Fund. Math. 47* (1959) 57–103.
[2] G. HIGMAN: Subgroups of finitely presented groups, Proc. Roy. *Soc. London (A) 262* (1961) 455–475.
[3] I. KAPLANSKY: *Infinite Abelian Groups*. (Univ. of Michigan Press, Ann Arbor 1954).
[4] G. T. KOZLOV and A. I. KOKORIN: Elementary theory of abelian groups without torsion, with a predicate selecting a subgroup, *Algebra and Logic 8* (1969) 182–190.
[5] J. R. SHOENFIELD: *Mathematical Logic*. (Addison-Wesley, Reading, Mass., 1967).

(Oblatum 26–VII–1974)

Department of Mathematics
Yale University
Box, 2155, Yale Station
New Haven, Conn. 06520
USA